UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/560,972	12/15/2005	Steven Charles Rhoads	PU030223	2440

7590 12/05/2007

Joseph S Tripoli
Thomson Licensing Inc
Patent Operations
P O BOx 5312
Princeton, NJ 08543-5312

EXAMINER	
HAILU, TESHOME	
ART UNIT	**PAPER NUMBER**
2139	

MAIL DATE	DELIVERY MODE
12/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/560,972	RHOADS, STEVEN CHARLES	
	Examiner	Art Unit	
	Teshome Hailu	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 are pending.

Claim Objections

2. Claims 4, 17 and 19 are objected to because of the information: the information "known, preloaded, pre-determined, determinable" is unclear. The examiner interprets this information as a "value" for examining purpose. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-24 are rejected under 35 U.S.C. 102(e) as being anticipated by Peyravian et al (Peyravian), US Pub. 2004/0158715.

As per claim 1, Peyravian discloses:

A device, located at a remote site on a network having a plurality of remote sites, for validating the source of an information item transmitted over said network, said device comprising: (Abstract, line 1-8, Peyravian teaches about the method of exchanging and authenticating public cryptographic keys between parties).

A processor in communication with a memory, said processor operable to execute code for: (paragraph 33, Peyravian disclosed about the server that distribute a public cryptographic key and

random generated password to a client using mail, email or telephone). Randomly generating a password inherently indicates that the server includes a processor and memory in order to perform the necessary steps.

Determining a first comparator value in relation to a first value associated with said information item received over said network and a Diffie-Hellman public key; (paragraph 35, Peyravian teaches the steps of generating a Diffie-Hellman public key Ds of the server. The server then provide an argument (ARGs) using public key and some other keys like client ID, prime modulus, secret key. Then the server hashes the generated argument (ARGs) to provide a hashed value as Hash(ARGs). At the end the server forms an extended concatenation using the hash argument, ID, cryptographic key and Diffie-Hellman public key then sends the extended concatenation EXTs to the client). Also see fig. 1, steps 150,155, 160 and 165.

Determining a second comparator value in relation to a digital signature received, said digital signature determined in association with a second value associated with said information item prior to transmission over said network; (paragraph 36-37, after receiving the extended concatenation EXTs, the client forms a concatenation argument ARGs' using public key and some other keys like ID, client secret key. Then the client hashes the generated argument (ARGs') to provide a hashed value as Hash(ARGs')). Also see steps 200, 205, 210 and 215 of fig. 2.

Comparing said first and second comparator values and validating said source based on said comparison. (Paragraph 37, Peyravian teaches that the client, after generating a hashed argument, compares the received hashed value Hash(ARGs) from the server with Hash(ARGs'). The client accepts the server information only if a positive result found. if the comparing result is not the same the client reject the information sent by the server). Also see steps 220, 225 and 230 of fig. 2.

As per claim 2, Peyravian discloses:

The device as recited in claim 1, wherein said processor is further operable to execute code for

determining said first value as a hash value of said received information items. (Paragraph 11, according to Peyravian, the server generates and sends a hashed value to the client).

As per claim 3, Peyravian discloses:

The device as recited in claim 1, wherein said public key is in the form of gxz mod(n) wherein g, x, z, and n are randomly selected large numbers and n is a prime number. (Paragraph 35, the server raise the password PW, random number, to the power Rs, which also a random number and reduces the result by modulo to form a diffie-Hellman public key Ds and denoted as Ds = PW *to the power of* Rs mod(p), where p is a prime number). Also see fig.2 step 140.

As per claim 4, Peyravian discloses:

The device as recited in claim 3, wherein said public key is selected from the group consisting of: known, preloaded, pre-determined, determinable. (Paragraph 11, according to Peyravian, the client generates a random number, prime value and computes a public key using a common password and sends the public key and prime value to the server prior to authentication). Also see steps 100-125 of fig. 1.

As per claim 5, Peyravian discloses:

The device as recited in claim 3, wherein said processor is operable to read said public key from an external media consisting of: magnetic tape, optic, memory. (Paragraph 11, Peyravian teaches that the client send Diffie-Hellman public key and the prime value to the server and the server generates a second Diffie-Hellman public key by reading the first Diffie-Hellman key and prime value send by the client).

As per claim 6 Peyravian discloses:

The device as recited in claim 3, wherein said processor is operable to execute code for receiving selected ones of said randomly selected large numbers over said network. (Paragraph 11, Peyravian teaches that the client send Diffie-Hellman public key and the prime value to the server and the server generates a second Diffie-Hellman public key by reading the first Diffie-Hellman key and prime value send by the client).

As per claim 7 Peyravian discloses:

The device as recited in claim 1, wherein said processor is further operable to execute code for receiving said public key over said network. (Paragraph 34, according to Peyravian, the client generates client ID, Diffie-Hellman public key and the prime value and sends them to the server). The client and server communication inherently indicates that there is a network connection between the server and client. Also receiving a message form the client inherently shows that there is a processor in the server.

As per claim 8 Peyravian discloses:

The device as recited in claim 3, wherein said processor is further operable to obtain selected ones of said randomly selected large numbers from preloaded sources from the group consisting of: magnetic tape, optic medium, memory. (Paragraph 11, the client generates a first random number, prime value and Diffie-Hellman public key using a password). Further Peyravian teach (paragraph 34, according to Peyravian, the client generates client ID, Diffie-Hellman public key and the prime value from random value and sends them to the server).

As per claim 9 Peyravian discloses:

The device as recited in claim 1, further comprising: an I/O unit in communication with said processor and said network. (Paragraph 16, Peyravian teaches about client as a user machine and the server is a service provider machine). Further the invention of Peyravian is about the communication

between server and client which inherently indicate that there is an I/O unit in communication with processor.

As per claim 10 Peyravian discloses:

The device as recited in claim 9, wherein said I/O unit is further in communication with said memory. (Paragraph 16, Peyravian teaches about client as a user machine and the server is a service provider machine). Further the invention of Peyravian is about the communication between server and client which inherently indicate that there is an I/O unit in communication with memory.

As per claim 11 Peyravian discloses:

The device as recited in claim 1, wherein said code is stored in said memory. ((Paragraph 16, Peyravian teaches about client as a user machine and the server is a service provider machine). Further Peyravian claimed a program storage device on claim 1 and claim 11.

As per claim 12 Peyravian discloses:

The device as recited in claim 1, wherein said second value is a hash value. (Paragraph 36-37, the client forms a concatenation argument ARGs' using public key and some other keys like ID, client secret key. Then the client hashes the generated argument (ARGs') to provide a hashed value as Hash(ARGs')).

As per claim 13 Peyravian discloses:

The device as recited in claim 1, wherein said source is validated when said first and second comparator values are equal. (Paragraph 37, Peyravian teaches that the client, after generating a hashed argument, compares the received hashed value Hash(ARGs) from the server with Hash(ARGs'). The

client accepts the server information only if a positive result found. if the comparing result is not the same the client reject the information sent by the server). Also see steps 220, 225 and 230 of fig. 2.

As per claim 14 Peyravian discloses:

A method for validating the source of an information item transmitted over a network, said method comprising the steps of: determining a first comparator value in relation to a first value associated with said information item transmitted over said network and a Diffie-Hellman public key; (paragraph 35, Peyravian teaches the steps of generating a Diffie-Hellman public key Ds of the server. The server then provide an argument (ARGs) using public key and some other keys like client ID, prime modulus, secret key. Then the server hashes the generated argument (ARGs) to provide a hashed value as Hash(ARGs). At the end the server forms an extended concatenation using the hash argument, ID, cryptographic key and Diffie-Hellman public key then sends the extended concatenation EXTs to the client). Also see fig. 1, steps 150,155, 160 and 165.

Determining a second comparator value in relation to a digital signature, wherein said digital signature is associated with said information items prior to transmission over said network; (paragraph 36-37, after receiving the extended concatenation EXTs, the client forms a concatenation argument ARGs' using public key and some other keys like ID, client secret key. Then the client hashes the generated argument (ARGs') to provide a hashed value as Hash(ARGs')). Also see steps 200, 205, 210 and 215 of fig. 2.

Comparing said first and second comparator values and validating said source based on said comparison. (Paragraph 37, Peyravian teaches that the client, after generating a hashed argument, compares the received hashed value Hash(ARGs) from the server with Hash(ARGs'). The client accepts the server information only if a positive result found. if the comparing result is not the same the client reject the information sent by the server). Also see steps 220, 225 and 230 of fig. 2.

As per claim 15 Peyravian discloses:

The method as recited in claim 14, further comprising the step of: determining said first value as a hash value of said information items. (Paragraph 11, according to Peyravian, the server generates and sends a hashed value to the client).

As per claim 16 Peyravian discloses:

The method as recited in claim 14, wherein said public key is in the form of: gxz mod(n) wherein g, x, z, and n are said randomly selected large numbers and n is a prime number. (Paragraph 35, the server raise the password PW, random number, to the power Rs, which also a random number and reduces the result by modulo to form a diffie-Hellman public key Ds and denoted as Ds = PW ^ Rs mod(p), where p is a prime number). Also see fig.2 step 140.

As per claim 17 Peyravian discloses:

The method as recited in claim 16, wherein said pubic key is selected from the group consisting of: known, preloaded, predetermined, determinable. (Paragraph 11, according to Peyravian, the client generates a random number, prime value and computes a public key using a common password and send the public key and prime value to the server prior to authentication). Also see steps 100-125 of fig. 1.

As per claim 18 Peyravian discloses:

The method as recited in claim 16, wherein said public key is transmitted over said network. (Paragraph 11, Peyravian teaches that the server send Diffie-Hellman public key to the client). The communication between the server and client inherently indicates that there is a network connection between them.

As per claim 19 Peyravian discloses:

The method as recited in claim 16, wherein selected ones of said large number values are

selected from the group consisting of: known, preloaded, predetermined. (Paragraph 11, according to Peyravian, the client generates a random number, prime value and computes a public key using a common password and sends them to the server prior to authentication). Also see steps 100-125 of fig. 1.

As per claim 20 Peyravian discloses:

The method as recited in claim 16, wherein selected ones of said large number values are received from said network. (Paragraph 11, Peyravian teaches that the client send Diffie-Hellman public key and the prime value to the server). The communication between the server and client inherently indicates that there is a network connection between them.

As per claim 21 Peyravian discloses:

The method as recited in claim 14, wherein said source is validated when said first and second comparator values are equal. (Paragraph 37, Peyravian teaches that the client, after generating a hashed argument, compares the received hashed value Hash(ARGs) from the server with Hash(ARGs'). The client accepts the server information only if a positive result found. if the comparing result is not the same the client reject the information sent by the server). Also see steps 220, 225 and 230 of fig. 2.

As per claim 22 Peyravian discloses:

A device for generating digital signatures comprising: a processor in communication with a memory, said processor operable to execute code for: (paragraph 33, Peyravian disclosed about the server that distribute a public cryptographic key and random generated password to a client using mail, email or telephone. Randomly generating a password inherently indicates that the server includes a processor and memory in order to perform the step).

Generating a first and second Diffie-Hellman public key from a plurality of large numbers randomly selected, wherein at least one of said numbers is a prime number; determining a public key as a Diffie-Hellman transpose of one of said Diffie-Hellman public keys. (paragraph 11, Peyravian teaches

that the client computes a first Diffie-Hellman public using random generated number and prime value. The client then sends the first Diffie-Hellman public key and prime value to the server so that the server can generate a second Diffie-Hellman public key).

As per claim 23 Peyravian discloses:

The device as recited in claim 22, further comprising: a device in communication with said processor, said device operable to transmit said public key and a remaining one of said Diffie-Hellman public keys to an external device. (Paragraph 12, the server sends the public cryptograph key, the second Diffie-Hellman public key and the hashed value to the client).

As per claim 24 Peyravian discloses:

The device as recited in claim 23, wherein said external device is selected from the group consisting of: a network, a magnetic medium, an optical medium, human-readable media. (The communication between parties to share a common but secret password inherently indicates that there is a network connection between the parties).

Conclusion

5. The prior art made or record and not relied upon is considered pertinent to applicant's disclosure.

TITLE: System and Method of providing communication security, US Pub. No. 2002/0062451.

TITLE: Cryptographic Communication process and apparatus, US 6,075,865.

TITLE: Cryptographic key split combiner, US 6,885,747.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Teshome Hailu whose telephone number is (571) 270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Teshome Hailu

November 27, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100